Remarks

Claims 1-28 are presented for reconsideration, with claims 1, 14, 21, 27, and 28 being the independent claims. A corrected drawing sheet is provided to correct a typographical error in Figure 3. Claims 1-28 are amended for clarification. Paragraph [0001] of the specification has been updated to identify the cross-reference to a related application using a US serial number instead of an attorney docket number.

These changes are believed not to introduce any new matter, and their entry is respectfully requested.

Based on the above amendments and the following remarks, Applicants respectfully request that the Examiner reconsider all outstanding rejections and that they be withdrawn.

Objections to the Drawings

The Applicants have amended FIG. 3 in the concurrently attached replacement sheet to accommodate the Examiner's request. The correction is made in compliance with 37 C.F.R. § 1.121(d) to correct FIG. 3 to correspond to the description of FIG. 3 provided in the originally filed specification. The correction to FIG. 3 does not add new matter. Support for this amendment can be found in paragraph 56 of the Applicants' specification. Accordingly, Applicants respectfully request that this amendment be entered.

Objections under 37 C.F.R. § 1.75(a)

On page 3 of the Office Action, the Examiner objected to claim 17 as failing to particularly point out and distinctly claim the subject matter which Applicants regard as their invention pursuant to 37 C.F.R. § 1.75(a). The Applicants have amended claim 17

to overcome this objection. This amendment does not narrow the scope of protection. Accordingly, Applicants respectfully request that the Examiner withdraw this objection of claim 17 and find it allowable.

Rejections under 35 U.S.C. § 101

On pages 4 and 5of the Office Action, the Examiner rejected claims 1-20, 27, and 28 under 35 U.S.C. § 101 for being directed to non-statutory subject matter. Applicants respectfully traverse these rejections.

On page 4 of the Office Action, the Examiner makes the conclusory statement that claims 1-20 are "directed towards software alone" and "nothing more than software modules doing different tasks of the claimed system or method." Applicants respectfully disagree. Applicants assert that the Examiner has misunderstood the Applicants' specification, embodiments, and computer readable medium examples. Applicants further assert that the Examiner has misapplied the guidelines in making 35 U.S.C. § 101 rejections of claims 1-20. Page 17 of the USPTO "Interim Guidelines for Examination of Patent Applications for Patent Subject Matter Eligibility" (Official Gazette notice of 22 November 2005), Section IV. C. reads as follows:

> "While abstract ideas, natural phenomena, and laws of nature are not eligible for patenting, *methods* and products employing abstract ideas, natural phenomena, and laws of nature to perform a real-world function may well be." (Emphasis added)

On page 4 of the Office Action, the Examiner concedes that claims 1-20 are directed to systems and methods, but asserts that Applicants' specification "provides intrinsic evidence that these claims are directed towards software alone." The Examiner seems to have misunderstood embodiments in Applicants' specification and what is claimed in claims 1-20. Paragraphs 11-20 and 36-47 of Applicants' specification provide

support for the document security systems and methods claimed in claims 1-20. Claims 1-20 are directed towards a document security system and methods, not "software alone," and represent statutory subject matter. While paragraphs 20 and 21 of Applicants' specification disclose computer readable media including computer program code for implementing document security methods as claimed in claims 27 and 28, paragraphs 11-20 and 36-47 of the specification disclose document security systems and methods as claimed in claims 1-20.

On page 5 of the Office Action, the Examiner rejected claims 27 and 28 as being allegedly directed towards non-statutory subject matter. The Examiner concedes on page 5 of the Office Action that claims 27 and 28 would normally be statutory. On page 6 of the Office Action, the Examiner objected to the inclusion of a non-statutory example of computer readable media, carrier waves, in paragraph 56 of Applicants' specification. Although Applicants believe claims 27 and 28 represent patentable subject matter as currently pending in the application, Applicants have amended claims 27 and 28 to be directed towards *tangible* computer readable media to accommodate the Examiner's request (Emphasis added). Pursuant to the Examiner's suggestions on pages 6 and 7 of the Office Action, Applicants have amended claims 27 and 28 to further recite tangible computer readable media that include computer program code which, when executed by a computer, causes the computer to perform steps and actions. In 1995, the Commissioner of Patents and Trademarks conceded to the U.S. Court of Appeals for the Federal Circuit "that computer programs embodied in a tangible medium, such as floppy diskettes, are patentable subject matter under 35 U.S.C. § 101." See *In re Beauregard*,

53 F.3d 1583 (Fed. Cir. 1995). Amended claims 27 and 28 fall within what the Commissioner of Patents and Trademarks had conceded was patentable subject matter.

Rejections under 35 U.S.C. § 102

On pages 6 and 7 of the Office Action, the Examiner rejected claims 1-9, 14-17, and 27 under 35 U.S.C. § 102(e) as being allegedly unpatentable in view of US Patent Application 2004/0117371 to Bhide *et al* (20040117371 A1) ("Bhide").

Claims 1-9

Applicants respectfully submit that Bhide does not describe each and every element as set forth in claims 1-9. For example, claim 1 recites a document security system comprising at least one process-driven security policy that includes states with access restrictions and transition rules specifying when a secured document transitions from one state to another. Claim 1 also recites an access manager that determines whether access to a secured document is permitted by a requestor based on the state and the corresponding access restrictions.

On page 7 of the Office Action, the Examiner indicates that claim 1's document security system is anticipated by paragraphs 1, 3, 21, 23, and 25 of Bhide. Applicants respectfully disagree. Applicants have examined the cited paragraphs of Bhide and are unable to identify a teaching of transition rules used to transition secured documents from state to state as recited in claim 1. Applicants' claim 1 recites secured documents transitioning from one state to another based upon process-driven security policy states with defined access restrictions and transition rules. Bhide infers database access privileges for access requests when no explicit privileges exist (Bhide, paragraph [0009],

lns. 1-3) and lacks any teaching of transition rules for secured documents. Bhide is limited to inferring user insert, delete, modify, or read access to portions of a database or basing database insert, delete, modify, or read access upon events (Bhide, paragraph [0028], lns. 1-19). Bhide does not teach or suggest securing or encrypting documents based upon process-driven security policy states that have specified access restrictions and transition rules as recited in Applicants' claim 1. Bhide's event-based database access is limited to insertion, deletion, modification, and reading of portions of a database (Bhide, paragraph [0028], lns. 1-6) and lacks claim 1's recited features of a process-driven file security system that determines access to secured documents.

As disclosed in paragraph 37 of Applicants' specification, the secured document recited in claim 1 can be various types of documents, multimedia files, data, executable code, images, text, or a collection of files. Paragraph 37 of Applicants' specification defines a secured document as an electronic file stored or presented in a form that is nearly impossible to read without authorization and authentication. As disclosed in paragraph 42 of Applicants' specification, secured documents recited in claim 1 require one or more keys, passwords, or access privileges to gain access to their content and security is provided through encryption and access rules. Applicants are unable to find any teaching in Bhide of a document security system that protects files, executable code, or images. Applicants are also unable to identify any teaching in Bhide of a document security system that protects secured files with keys or encryption as recited in claim 1 and disclosed in Applicants' specification. Bhide is limited to event-based access control of databases (paragraph [0018], lns. 1-4, paragraph [0028], lns. 1-6) and allows users to

gain one of three database access privileges: read, write, or indirect read (Bhide, paragraph [0012], lns. 1-4).

On page 8 of the Office Action, the Examiner indicates that the above-recited access manager of claim 1 is disclosed by Bhide in lines 3-10 of paragraph 31 which read:

> "The Execution Model 44 detects the occurrence of events. It also checks the truth-value of the conditions attached to the policies and depending on the truth-value, it executes the inference rules 18 as well as the access enforcement part 20 of the policy 10. The Access Validation model 46, provides an interface to the end-users 52 to access data from the underlying databases or information repositories 54."

Applicants have examined lines 3-10 of paragraph 31 of Bhide and are unable to identify teaching of an access manager that determines whether access to a secured document is permitted by a requestor based on the process-driven security policy's state and the corresponding access restrictions for the secured document as recited in claim 1. It appears as if the Examiner is indicating that Bhide's "Execution Model" and "Access Validation model" accomplish claim 1's recited access manager features of determining secured document access based upon transition rules. Although Bhide's Access Validation model provides an end-user interface for accessing data once database access has been inferred by the Execution Model, Applicants assert that database access via a user interface is not analogous to determining whether access to a secured document is permitted by a requestor based on a process-driven security policy's current state and corresponding access restrictions. Even assuming the Examiner's interpretation is correct, which Applicants disagree with, Applicants assert that while Bhide may disclose inferring database access based upon conditions attached to database access policies

(Bhide, paragraph [0031], lns. 4-8), Bhide does not teach use of an access manager to determine a requestor's access to secured documents as recited in claim 1.

Therefore, the applied reference does not anticipate claim 1. Also, at least based on their respective dependencies to claim 1, claims 2-9 should be found allowable, as well as for their additional respective distinguishing features. Accordingly, Applicants respectfully request that the Examiner reconsider and withdraw the rejections of these claims, and find them allowable over the applied reference.

Claims 14-17

Applicants respectfully submit that Bhide does not describe each and every element as set forth in claims 14-17. For example, claim 14 recites a method for transitioning a secured document through a security-policy state machine having a plurality of states. Claim 14 further recites that the method includes receiving an event, determining whether the event causes a state transition for the secured document from a former state to a subsequent state, and automatically transitioning from the former state to the subsequent state of the security-policy state machine when it is determined that the event causes the state transition.

On page 11 of the Office Action, the Examiner indicates that Bhide discloses the above-recited features of claim 14 in paragraphs 3, 18, 21, and 24. Applicants respectfully disagree. Applicants have examined paragraphs 3, 18, 21, and 24 of Bhide and are unable to find any teaching of transitioning a secured document through a security policy state machine as recited in claim 14. As argued above, Bhide is limited to controlling user access to databases and does not disclose or suggest changing states

of secured documents. Although Bhide may disclose that conditions can trigger enforcement of database access control privileges (Bhide, paragraph [0021], lns. 1-5), Bhide does not change the security state of a document based on events as recited in Applicants' claim 14. Bhide's alteration of database access rules is not analogous to transitioning a secured document through a security policy state machine as recited in claim 14.

Bhide also lacks claim 14's recited step of automatically transitioning a secured document's state from a former state to a subsequent state in a security-policy state machine when an event causes a state transition. Bhide infers database access rules based on conditions and applies rules to data related to access control, user hierarchy, and user profiles (Bhide, paragraph [0024], lns. 1-3). Bhide's access control rules are executed or enforced only if the associated condition is true (Bhide, paragraph [0024], lns. 4-6), and Bhide does not automatically transition a document's security state based on events as recited in claim 14.

Therefore, the applied reference does not anticipate claim 14. Also, at least based on their respective dependencies to claim 14, claims 15-17 should be found allowable, as well as for their additional respective distinguishing features. Accordingly, Applicants respectfully request that the Examiner reconsider and withdraw the rejections of these claims, and find them allowable over the applied reference.

Claim 27

Applicants respectfully submit that Bhide does not describe each and every element as set forth in claim 27. Claim 27 recites a combination of features that are not

found in the applied reference. For example, claim 27 recites a tangible computer readable medium that includes computer program code for transitioning secured documents through a security-policy state machine. As recited in claim 27, the tangible computer readable medium includes computer code, which when executed by a computer, causes the computer to detect occurrence of an event and determine whether the event causes a state transition for a secured document from a former state to a subsequent state of the security-policy state machine. Claim 27 also further recites a tangible computer readable medium that includes computer code that, when executed by a computer, automatically transitions from a former state to a subsequent state of the security-policy state machine upon determining that the event causes the state transition.

On page 13 of the Office Action, the Examiner indicates that Bhide discloses all of the above-recited features of claim 27 under the same rationale used to reject claim 14. Applicants respectfully disagree. Although Bhide may disclose a computer program product for execution of event-based database access control with inference of data access rights (Bhide, paragraph [0018], lns. 1-4), Bhide does not teach or suggest a computer readable medium with program code for transitioning secured documents through a security-policy state machine. Applicants are unable to identify any disclosure in Bhide of computer code that automatically transitions a secured document from a former security state to a subsequent state in a security-policy state machine as recited in claim 27.

As disclosed in paragraph 37 of Applicants' specification, the secured documents recited in claim 27 can be multimedia files, data, executable code, images, or a collection of files. Paragraph 37 of Applicants' specification defines a secured document as an

electronic file stored or presented in a form that is nearly impossible to read without authorization and authentication. Paragraph 42 of Applicants' specification discloses that one or more keys, passwords, or access privileges are needed to access the secured documents recited in claim 27. As disclosed in paragraph 42 of Applicants' specification, access to secured documents recited in claim 27 is provided through encryption and access rules. Applicants are unable to find any teaching in Bhide of a computer readable medium with program code that protects files, executable code, or images. Applicants are also unable to identify any teaching in Bhide of a computer readable medium with computer code that protects secured files with keys or encryption as recited in claim 27 and disclosed in Applicants' specification. As argued above, Bhide discloses event-based access control for databases (Bhide, paragraph[0018], lns. 1-4, paragraph [0028], lns. 1-6) and is limited to allowing users to gain read, write, or indirect read access to portions of a database (Bhide, paragraph [0012], lns. 1-4).

Therefore, the applied reference does not anticipate claim 27. Accordingly, Applicants respectfully request that the Examiner reconsider and withdraw the rejection of this claim, and find it allowable over the applied reference.

Rejections under 35 U.S.C. § 103

Claim 10 is rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over Bhide in view of US Patent Application 2003/0217333 to Smith *et al* (US 2003/0217333 A1) ("Smith"). On page 14 of the Office Action, claims 11-13 and 18-20 stand rejected in view of Bhide and in further view of US patent 6,341,164 to Dilkie (US 6,341,164 B1) ("Dilkie"). On page 20 of the Office Action, claims 21-26 are rejected as

allegedly being unpatentable in view of Bhide and in further view of US patent 6,941,472 to Moriconi *et al* (US 6,941,472 B2) ("Moriconi") and in further view of US Patent Application 2004/0098580 to DeTreville (US 2004/0098580 A1) ("DeTreville").

Applicants respectfully traverse these rejections and requests that these rejections be withdrawn and the claims be passed to allowance.

Claim 10

On page 13 of the Office Action, the Examiner indicates that claim 10 is rejected as allegedly being obvious over Bhide in view of Smith. Claim 10 recites a combination of features that are not found in the applied references. For example, claim 10 recites a document security system as recited in claims 1 and 9 comprised of at least one process-driven security policy that includes states with transition rules specifying when a secured document transitions from one state to another, wherein the transition rules are based on events and are written in XML. On page 13 of the Office Action, the Examiner concedes that Bhide is silent about writing transition rules in XML as recited in claim 10, but indicates that Smith cures this deficiency of Bhide. Applicants respectfully disagree. Smith's system and method for allowing e-commerce providers to customize and personalize Web site content for each customer (Smith, paragraph [0007], lns. 1-5) is not analogous to the document security system recited in claim 10. Smith addresses specific problems associated with applying rules in order to personalize Web content provided to a user in a Web environment (Smith, paragraph [0029], lns. 1-4). Smith does not teach or disclose a file or document security system with transition rules written in XML that specify when a secured document transitions from one state to another as recited in

Applicants' claim 10. Although Smith may disclose using XML files to configure a rules-based engine for Web site personalization (Smith, paragraph [0027], lns. 19-23), Smith does not teach or suggest using XML to write document security state transition rules as recited in claim 10.

The Examiner's piecemeal assembly of parts of Bhide and Smith to cure the deficiencies in Bhide destroys the teaching of both of these references by making the systems/methods of operation unsatisfactory for their intended purposes and/or changing the systems/principles of operation. See M.P.E.P § 2143.01(V) and (VI). As Bhide allows inference of access privileges for access requests when no explicit privileges exist (Bhide, paragraph [0009], lns. 1-3), adding Bhide's privilege inference to Smith's method for allowing e-commerce providers to customize and personalize Web sites for specific customers would at least change Smith's principle of operation (Emphasis added). Similarly, as Bhide allows access rules to be inferred (Bhide, paragraph [0009], lns. 1-3) adding Smith's Web content personalization based on specified rules (Smith, paragraph [0029], lns. 1-4), would change Bhide's principle of operation.

None of the applied references individually anticipate claim 10 and they cannot be used in combination to establish a *prima facie* case of obviousness. Therefore, Bhide and Smith do not anticipate claim 10. Accordingly, Applicants respectfully request that the Examiner reconsider and withdraw the rejection of this claim, and find it allowable over the applied references.

Claims 11-13

Claims 11-13 recite a combination of features that are not found in the applied references. For example, claim 11 recites the document security system of claim 1 wherein events cause the state of the process-driven security policy for the secured document to transition from a previous state to a current state and the secured document is modified when the document's policy transitions. The applied references alone or in combination do not teach or suggest the document security system features recited in claim 11.

On page 14 of the Office Action, the Examiner concedes that Bhide does not teach modifying a secured document when the process-driven security policy for the document transitions from a previous state to the current state, but asserts that this deficiency is cured by Dilkie in lines 24 and 25 of column 3. Applicants respectfully disagree. Applicants have examined lines 24 and 25 of column 3 of Dilkie and are unable to identify a disclosure of modifying a secured document when a process-driven security policy transitions as recited in claim 11. While Dilkie may disclose determining "whether an improper or undesirable encryption key was used to encrypt encrypted data" and re-encrypting data with a different encryption process when an improper encryption key is detected (Dilkie, col. 3, lns. 23-27), Dilkie does not teach or suggest modifying a secured document based on a security policy state transition as recited in claim 11. Dilkie discloses re-encryption of files when the wrong encryption key was used to encrypt data (Dilkie, col. 3, lns. 23-27), but does not suggest modifying secured documents based on a process-driven security policy change as recited in Applicants' claim 11.

Therefore, Bhide and Dilkie do not anticipate claim 11. Also, at least based on their respective dependencies to claim 11, claims 12 and 13 should be found allowable, as well as for their additional respective distinguishing features. Accordingly, Applicants respectfully request that the Examiner reconsider and withdraw the rejections of these claims, and find them allowable over the applied references.

Claims 18-20

Claims 18-20 recite a combination of features that are not found in the applied references. For example, claim 18 recites the method for transitioning a secured document through a security-policy state machine from claim 14 where the transitioning includes modifying the secured document to reflect the subsequent state of the security-policy state machine. The applied references alone or in combination do not teach or suggest modifying a secured document to reflect a subsequent state of a security-policy state machine as recited in claim 18.

On page 17 of the Office Action, the Examiner concedes that Bhide does not teach modifying a secured document to reflect the subsequent state of the security-policy state machine as recited in Applicants' claim 18, but asserts that this deficiency is cured by Dilkie in lines 24 and 25 of column 3. Applicants respectfully disagree. Applicants have examined lines 24 and 25 of column 3 of Dilkie and submit that they do not teach or suggest modifying a secured document to reflect a security policy state transition as recited in claim 18. Dilkie's "apparatus and method for facilitating an encryption process" discloses re-encrypting data with a different encryption process when an improper encryption key is detected (Dilkie, col. 3, lns. 14-15 and lns. 23-27), but clearly

does not teach modifying a secured document based on security policy state transitions as recited in claim 18.

Claim 19 recites the method for transitioning a secured document through a security-policy state machine from claim 14 where the transitioning comprises: retrieving an encrypted file key from the secured document; decrypting, when permitted by the former state of the security-policy state machine, the key; subsequently encrypting the key in accordance with the subsequent state of the security-policy state machine; and storing the secured document which includes at least an encrypted data portion and the subsequently encrypted file key. On pages 17 and 18 of the Office Action, the Examiner concedes that Bhide does not teach encrypting a secured document's key in accordance with a subsequent state of the security-policy state machine as recited in Applicants' claim 19, but asserts that this deficiency is cured by Dilkie in lines 62 and 63 of column 3, lines 7 and 8 of column 4, and lines 11-21 of column 8. Applicants have examined lines 62 and 63 of column 3, lines 7 and 8 of column 4, and lines 11-21 of column 8 of Dilkie and submit that they do not teach or suggest modifying a secured document or encrypting an associated key in accordance with the subsequent state of the security-policy state machine as recited in claim 19. Although Dilkie may disclose deleting unnecessary header cryptographic key packages, compressing message data, obtaining the decryption key, decrypting message data, compressing data, and then re-encrypting the compressed data (Dilkie, col. 8, lns. 4-10); compression and encryption of data does not suggest encrypting a secured document's key in accordance with a subsequent state of a security-policy state machine as recited in claim 19.

Claim 20 recites the method for transitioning a secured document through a security-policy state machine from claim 14 where the transitioning comprises: retrieving an encrypted file key from the secured document; obtaining a private state key associated with the former state of the security-policy state machine; decrypting the encrypted file key using the private file key; obtaining a public state key associated with the subsequent state of the security-policy state machine; subsequently encrypting the file key in accordance with the public state key; and storing the document which includes at least an encrypted data portion and the encrypted key. On pages 18 and 19 of the Office Action, the Examiner concedes that Bhide does not teach the method for transitioning a secured document through a security-policy state machine method including the above-recited steps in Applicants' claim 20, but asserts that this deficiency is cured by Dilkie in lines 11-21 of column 8, lines 62 and 63 of column 3 and lines 7 and 8 of column 4. Applicants have examined the cited paragraphs in Dilkie and submit that they does not teach or suggest the above-recited features of claim 20. Although Dilkie may disclose obtaining a message's decryption key, decrypting message data, compressing data, and then re-encrypting the compressed data (Dilkie, col. 8, lns. 4-10), compression and encryption of data does not teach or suggest encrypting a secured document's file key in accordance with the corresponding public state key as recited in claim 20.

The Examiner's piecemeal assembly of parts of Bhide and Dilkie to cure the deficiencies in Bhide destroys the teaching of both of these references by making the systems/methods of operation unsatisfactory for their intended purposes and/or changing the systems/principles of operation. As Bhide allows inference of access privileges for

access requests when no explicit privileges exist (Bhide, paragraph [0009], lns. 1-3), adding Bhide's privilege inference to Dilkie's method for re-encryption of files when the wrong encryption key was used to encrypt data would at least change Dilkie's principle of operation. Similarly, as Bhide allows access rules to be inferred (Bhide, paragraph [0009], lns. 1-3) adding Dilkie's re-encryption of files based upon detecting specified encryption key conditions (Dilkie, col. 3, lns. 23-27), would change Bhide's principle of operation.

None of the applied references individually anticipate claims 11-13 or 18-20 and they cannot be used in combination to establish a *prima facie* case of obviousness. Therefore, the applied references do not anticipate claims 11-13 or 18-20. Accordingly, Applicants respectfully request that the Examiner reconsider and withdraw the rejection of these claims, and find them allowable over the applied references.

Claims 21-26

On page 20 of the Office Action, the Examiner indicated that claims 21-26 are unpatentable in view of Bhide and in further view Moriconi and in further view of DeTreville. Claim 21 recites a combination of features that are not found in the applied references. For example, claim 21 recites a method for imposing access restrictions on electronic documents comprising: providing at least one process-driven security policy at a server machine, the policy having a plurality of states that each have distinct access restrictions; providing a reference to the security policy at a client machine, the reference referring to the policy on a server; associating the reference with an electronic document; transitioning the policy from one state to a current state; and subsequently determining at the server whether a requestor is permitted to access the document based on a current

state of the policy, and informing the server of the current state by sending the reference to the server. On page 20 of the Office Action, the Examiner asserts that paragraph 21 of Bhide discloses the recited method of claim 21. Applicants respectfully disagree. Even assuming the Examiner's interpretation is correct, which Applicants disagree with, Applicants submits that the cited paragraph in Bhide only disclose an event-based access control system for databases (Bhide, paragraph [0003], lns. 4-7, paragraph [0031], ln. 1), and does not suggest the method including the above-recited steps of claim 21.

On page 21 of the Office Action, the Examiner acknowledges that Bhide does not teach providing a reference to a process-driven security policy at a client machine, the reference referring to the process-driven security policy residing on the server machine, and associating the reference with an electronic document as recited in claim 21, but asserts that these deficiencies of Bhide are cured by lines 22-26 of column 5 of Moriconi. Applicants have examined the cited lines 22-26 of column 5 of Moriconi and submit that they cannot be reasonably understood to teach the above-recited features of Applicants' claim 21. Moriconi is concerned with protecting computer systems against unauthorized access (Moriconi, col. 5, lns. 7-9). Moriconi discloses use of a "policy manager" which allows users to add and edit policy rules of a centrally-managed, global security policy (Moriconi, col. 8, lns. 65-67, col. 9, lns. 32-34). Although Moriconi may disclose a system for managing computer system security requirements with a policy manager on a server that manages and distributes a global security policy to clients (Moriconi, col. 5, lns. 19-26), Moriconi does not suggest providing references to clients for a process-driven security policy with a plurality of states as recited in claim 21. Moriconi is limited to security techniques and systems to protect computer systems against

unauthorized access (Moriconi, col. 5, lns. 7-9). Moriconi uses a global security policy distributed from a server to clients (Moriconi, col. 3, lns. 56-61, col. 5, lns. 21-23), and does not teach or suggest transitioning a security policy from one state to a current state as recited in claim 21. Applicants are unable to identify any disclosure of a process-driven security policy or transitioning a security policy from one state to a current state in Moriconi.

On page 22 of the Office Action, the Examiner concedes that the "combination of Bhide and Sames (sic - Moriconi) does not teach that the current state being informed to the server computer by sending the reference to the server", but asserts that this deficiency is cured by lines 1-4 of paragraph 24 of DeTreville. Applicants have examined lines 1-4 of paragraph 24 of DeTreville and are unable to identify a teaching of a client informing a server of a process-driven security policy state with distinct access restrictions as recited in claim 21. DeTreville is concerned with granting rights to resources by distributing and processing licenses (DeTreville, paragraph [0020], lns. 1-4, paragraph [0031], lns. 1-4). Although DeTreville discloses methods and systems for license processing with an access control module that requests current license state information from a state server (DeTreville, paragraph [0020], lns. 1-3, paragraph [0024], lns. 1-4), DeTreville's license states are external to licenses and do not change or transition the licenses (DeTreville, paragraph [0006], lns. 1-4, paragraph [0007], lns. 5-8). Changes in DeTreville's license states do not result in altered licenses, and are limited to controlling how many times or for how much time a resource can be accessed (DeTreville, paragraph [0004], lns. 1-6, paragraph [0020], lns. 9-12, paragraph [0024], lns. 12-17). DeTreville's license states are counters that are incremented or decremented

based on how many times or for how long a given resource is used or accessed (DeTreville, paragraph [0025], lns. 7-9, paragraph [0027], lns. 1-4, paragraph [0037], lns. 15-19), not security policies that are changed based on state transitions as recited in Applicants' claim 21. Applicants are unable to identify a teaching in DeTreville of a server being informed of a transitioned document security policy by a client as recited in Applicants' claim 21.

The Examiner's piecemeal assembly of parts of Bhide, Moriconi, and DeTreville to cure the deficiencies in Bhide destroys the teaching of both of these references by making the systems/methods of operation unsatisfactory for their intended purposes and/or changing the systems/principles of operation. See M.P.E.P § 2143.01(V) and (VI). As Bhide allows inference of access privileges for access requests when no explicit privileges exist (Bhide, paragraph [0009], lns. 1-3), adding Bhide's privilege *inference* to Moriconi's system with a *global* policy that *specifies* user access privileges for securable components (Moriconi, col. 3, lns. 62-63) would at least change Moriconi's principle of operation (Emphasis added). Similarly, as Bhide allows access rules to be inferred (Bhide, paragraph [0009], lns. 1-3) adding Moriconi's system with a global security policy specifying access privileges (Moriconi, col. 3, lns. 57-59) would change Bhide's principle of operation. DeTreville's methods and systems for license processing are not analogous to Bhide's database access privileges or Moriconi's system for managing computer system security requirements.

None of the applied references individually anticipate claim 21 and they cannot be used in combination to establish a *prima facie* case of obviousness. Also, at least based on their respective dependencies to claim 21, claims 22-26 should be found

allowable, as well as for their additional respective distinguishing features. Therefore, the applied references do not anticipate claims 21-26. Accordingly, Applicants respectfully request that the Examiner reconsider and withdraw the rejections of these claims, and find them allowable over the applied references.

Conclusion

All of the stated grounds of rejection have been properly traversed, accommodated, or rendered moot. Applicants therefore respectfully request that the Examiner reconsider all presently outstanding rejections and that they be withdrawn. Applicants believe that a full and complete reply has been made to the outstanding Office Action and, as such, the present application is in condition for allowance. If the Examiner believes, for any reason, that personal communication will expedite prosecution of this application, the Examiner is invited to telephone the undersigned at the number provided.

Prompt and favorable consideration of this Amendment and Reply is respectfully requested.

Respectfully submitted,

STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.

Glenn J. Perry
Attorney for Applicant
Registration No. 28,458

Date: June 18, 2007

1100 New York Avenue, N.W.
Washington, D.C. 20005-3934
(202) 371-2600

682975_5.DOC